

PHASE 1 READINESS

Bring the owners, the real system, and one complete customer journey.

This workbook defines the minimum information and people required to turn Phase 1 into a decision-ready architecture and implementation plan within ten business days.

01

People

Named decision owners with authority to resolve product, technical, security, and commercial questions.

02

Systems

Relevant code, AWS topology, APIs, current agents, checkout SDK, data, and operational controls.

03

Proof

One representative customer journey, real failure examples, and measurable acceptance criteria.

NAME THE OWNERS

Every unresolved question needs one accountable decision owner.

ROLE	RESPONSIBILITY	NAME	AVAILABILITY
Executive sponsor	Outcome, budget, scope, escalation, final acceptance	Yash Daftary	_____
Product owner	Customer journeys, admin experience, roadmap, priorities	Alisha Mody	_____
Technical owner	Codebase, APIs, identity, integration, implementation constraints	Bhavin or delegate	_____
AWS/security owner	Cloud boundary, IAM, network, logs, compliance, access approval	_____	_____
Checkout SDK owner	Third-party embed flow, keys, publishing, supported patterns	_____	_____
AI/agent owner	Current agents, prompts, tools, evaluations, failure cases	_____	_____

Decisions to make during Phase 1

- ✓ First use case and smallest useful publishable outcome
- ✓ Organization, workspace, studio, and user mapping
- ✓ Commas AWS placement and operational ownership
- ✓ Human approval and prohibited-action policy
- ✓ Cross-tenant learning signals that may be aggregated
- ✓ Phase 2 option and pilot acceptance criteria

MINIMUM VIABLE ACCESS

Start read-only. Escalate only when the finding requires it.

Product package

- ✓ Product map and current roadmap
- ✓ New creator journey
- ✓ Existing-business journey
- ✓ Admin and compliance journey
- ✓ Embedded checkout SDK flow
- ✓ Representative support and failure examples

Technical package

- ✓ Relevant read-only repositories
- ✓ Architecture and service map
- ✓ Authentication and tenancy model
- ✓ Current agent implementation
- ✓ Internal API and webhook docs
- ✓ Deployment and environment overview

AWS and security

- ✓ Account and environment topology
- ✓ Network and IAM model
- ✓ Secrets and key-management approach
- ✓ Logging, incident, and audit expectations
- ✓ Data classification and retention
- ✓ Approved AI/model providers

Evaluation evidence

- ✓ Current performance metrics
- ✓ Known unsafe or prohibited behaviors
- ✓ Prompt and tool failure examples
- ✓ Representative synthetic profiles
- ✓ Conversion and completion definitions
- ✓ Customer-isolation requirements

Do not send in email: passwords, API keys, production credentials, customer payment information, regulated data, or raw production exports. MIOSA will provide the approved access path after kickoff.

OPEN THE WORKING LANE

Give MIOSA a secure path to the code and the people who operate it.

GITHUB ACCESS

Add Roberto to the relevant repositories

GitHub: @robertohluna

Email: roberto@miosa.ai

- ✓ Read access to all repositories required for Phase 1 discovery
- ✓ Visibility into relevant issues, pull requests, branches, and technical documentation
- ✓ Repository list with a one-line purpose and named owner for each
- ✓ Write access only if later approved for a bounded implementation task

COMMUNICATION

Create one direct technical channel

Open a shared Slack channel or equivalent thread that includes the Commas product owner, technical owner, relevant development leads, and Roberto.

- ✓ Use it for architecture questions, access blockers, decisions, and meeting follow-ups
- ✓ Name one person responsible for routing unanswered questions
- ✓ Keep credentials and sensitive customer data out of chat
- ✓ Record material decisions in the Phase 1 decision log

CODEBASE WALKTHROUGH

Schedule a technical onboarding call

A Commas engineer should walk MIOSA through the relevant repository or repositories, the local development path, and the production boundary.

- ✓ Service ownership and repository relationships
- ✓ Authentication, organizations, workspaces, and tenant isolation
- ✓ Current agents, prompts, tools, models, and evaluation path
- ✓ APIs, SDKs, webhooks, queues, and official state
- ✓ Build, test, deployment, observability, and incident workflow

SECURE ACCESS

Grant the minimum useful access

Begin with source access and nonproduction documentation. Expand access only when a discovery finding requires it and the responsible Commas owner approves it.

- ✓ Use Commas-managed invitations and least-privilege roles
- ✓ Prefer nonproduction or read-only cloud views for architecture discovery
- ✓ Share secrets through an approved secrets manager, never email
- ✓ Confirm access removal and data return or destruction at closeout if Phase 2 does not proceed

Completion condition: MIOSA can inspect the relevant code, reproduce the supported local path, identify the owners of each service, and ask implementation questions in a channel where the responsible Commas team can answer them.

ONE FLOW END TO END

Describe the first use case in operating terms.

USER	Who performs the work? What do they know? What can they approve?
TRIGGER	What event or intent starts the journey?
INPUTS	What facts, files, answers, APIs, and business context are required?
PROCESS	What does the agent plan, create, verify, and hand off?
OUTPUT	What exactly becomes reviewable and publishable?
OFFICIAL STATE	What is written back into Commas after approval?
POLICY GATES	What is prohibited, flagged, rate-limited, or escalated?
EVIDENCE	What proves what happened and why?
OUTCOME	What business result is observed later?
SUCCESS	What completion, quality, cost, safety, and performance thresholds matter?

Recommended session artifact: bring one current customer example from initial intent through a live or failed outcome, including the manual work Commas performs today.

90-MINUTE WORKING SESSION

Leave kickoff with owners, access, and a bounded proof.

00-15 MIN

Outcome and constraints

Confirm Phase 1 decision, first use case, non-goals, commercial concerns, and immovable product or compliance rules.

15-35 MIN

Customer journey

Walk the new-creator and embedded-checkout flows. Select the proof and name its success measures.

35-60 MIN

System and tenant map

Review Commas services, identity, org/workspace model, AWS, current agents, APIs, and official state.

60-75 MIN

Data and control boundary

Define allowed data, secrets, approvals, hard prohibitions, cross-tenant learning, and incident expectations.

75-90 MIN

Readiness and schedule

Confirm owners, access, working sessions, midpoint checkpoint, Miami review, blockers, and next action.

OUTPUT

Signed operating brief

Named use case, owner map, access register, decision log, known risks, and the Phase 1 execution calendar.